UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------x

ERIC HU,
on behalf of himself and others similarly situated,
Plaintiff,

v.

WHALECO, INC.
d/b/a Temu,
Defendant.

----------x

Case No. 23-cv-06962

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff ERIC HU ("Plaintiff" or "Hu") brings this Class Action Complaint against Defendant WHALECO, INC. d/b/a Temu ("Defendant" or "Temu"), on behalf of himself and others similarly situated, and complains and alleges upon personal knowledge as to himself and his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys:

NATURE OF THE ACTION

1. Plaintiff brings the proposed class action against Defendant on behalf of all persons who downloaded Temu, an application (the "Temu app"), and used Temu's in-app website browser ("in-app browser").

2. Plaintiff brings this proposed class action against Defendant for its failure to secure and safeguard its customers' personal data, including name, address, email address, phone number, financial information (credit card information) and biometrics data (fingerprinting), enabling hackers to steal personal and financial data from Defendant and put Class members' personal and financial information at serious and ongoing risk (the "Data Breaches" or "Breaches").

3. The Breaches were caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. Defendant grossly failed to comply with security standards and allowed its customers'

financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Breach.

4. The Breaches, as complained of and reported to the Better Business Bureau, include multiple reports of credit card information and bank information being sold or leaked after use on Temu.

5. The hackers continue to use the information they obtained as a result of Defendant's inadequate security to exploit and injure Class members across the United States.

6. Defendant failed to uncover and disclose the extent of the Breach and notify its affected customers of the Breach in a timely manner. Defendant failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Breaches. Furthermore, by failing to provide adequate notice, Defendant prevented Class members from protecting themselves from the Breaches.

7. Plaintiff further brings this proposed class action against Defendant for wiretapping the electronic communications of visitors to its website, www.temu.com.

8. As described more fully below, the in-app browser inserts JavaScript code into the website visited by Temu users. The clear purpose of the JavaScript code inserted into these websites is to track every detail about Temu users' website activity.

9. Through the use of its in-app browser, Temu has secretly and invasively amassed massive amounts of extremely private information and data about its users by tracking their activity on third-party websites. Defendants have unlawfully intercepted private and personally identifiable data and content from Temu users so that Defendants may generate revenue from use of this data. Through their clandestine tracking activities, Defendants have violated wiretap laws, unlawfully intruded upon users' privacy, violated their rights of privacy, and unjustly profited from

their unlawful activities.

10. Congress passed the Wiretap Act to protect the privacy of the people of the United States. The Wiretap Act is very clear in its prohibition against intentional unauthorized taping or interception of any wire, oral, or electronic communication. In addition to other relevant sections, the Wire Tap Act states that any person who: "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" has violated the act. 18 U.S.C. §2511.

11. Plaintiff brings this action for every violation of the Wiretap Act which provides for statutory damages of the greater of $10,000 or $100 per day for each violation of 18 U.S.C. §2510 *et seq.* under 18 U.S.C. §2520.

12. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for breach of implied contract and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

JURISDICTION & VENUE

13. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of other members of the class exceed $5,000,000.00 exclusive of interest and costs, and there are numerous Class members who are citizens of States other than Defendant's State of citizenship.

14. This Court has personal jurisdiction over Defendant because Defendant continuously and permanently does business in New York and has established the requisite minimum contacts with New York.

15. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2), as a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this

District.

PARTIES

PLAINTIFF ERIC HU

16. Hu is a citizen of the State of New York and is domiciled in Queens County, New York. Hu registered with Temu in about August 2023, and made purchases from Temu during that time. As a result, Hu entered into an implied contract with Temu for the adequate protection of his personal identifying information and had his personal identifying information exposed as a result of Defendant's inadequate security.

17. Hu downloaded the Temu app and created his Temu account on an Android mobile device.

18. While using the Temu app, Plaintiff clicked on links to external, third party websites where he completed his purchase and entered his private data, including his credit card information. Defendant surreptitiously collected data associated with Plaintiff's use of third party websites without his knowledge or consent, including his contact and credit card information provided during Plaintiff's purchase of merchandise.

DEFENDANT WHALECO INC d/b/a Temu

19. Defendant WHALECO INC d/b/a Temu is a Delaware business corporation with its principal place of business in Massachusetts, doing business in all 50 States and the District of Columbia.

20. Temu is at the vanguard of ultra-fast fashion, where technology and highly efficient supply chains meet to satisfy consumer demand for cutting-edge fashions at ultra-low prices. The speed of communications and rapidly changing consumer preferences and fashion have created strong consumer demand for the ultra-fast fashion business model.

21. Temu entered the U.S. market in or around July 2022, becoming U.S. consumers'

favorite ultra-fast retailer, topping the app store charts and consistently offering lower prices than Shein, its major competitor in the field.

22. On December 24, 2022, during the peak of the holiday shopping season in the U.S., *The Wall Street Journal*, published an article dedicated to a retailer that had entered the market only three months prior. "American Bargain Hunters Flock to a New Online Platform Forged in China" read the headline. The byline continued, "Temu, a marketplace with deep discounts and copious discounts, has become the most downloaded app in the U.S."

FACTUAL BACKGROUND

23. The unique characteristics of ultra-fashion requires market participants to act as e-commerce retailers, meaning all or virtually all of their sales come from online sales.

24. The products offered on the Temu Platform include men's, women's, and children's apparel. Like Shein, nearly all Temu's product offerings in the U.S. come from a network of manufacturers located in China.

WEBSITE USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR INTERACTIONS WITH WEBSITES

25. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[1]

26. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website visitors will assume their detailed interactions with a website will only be used by the website and not shared with a party

[1] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

they know nothing about. As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[2]

27. Privacy polls and studies show that a majority of Americans believe that internet companies and website should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of data that has been collected about them.[3]

28. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected by them by companies.[4]

A HERITAGE OF MALWARE

29. Temu is owned by PDD Holdings, Inc, which is headquartered in China.

30. PDD Holdings, Inc. also owns Pinduoduo, a shopping app known for selling everything from groceries to clothing.

31. Previously Pinduoduo was pulled from Google's app store due to the presence of malware that exploited vulnerabilities in the Android operating system to spy on users and competitors. [5]

32. In response to slowing increase in monthly users, Pinduoduo "set up a team of around 100 engineers and product managers to dig for vulnerabilities in Android phones, develop ways to exploit them—and turn that into profit." "By collecting expansive data on user activities,

---

[2] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[3] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[4] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/

[5] Reuters. "Google suspends China's Pinduoduo app on security concerns." (March 21, 2023). https://www.reuters.com/technology/google-suspends-chinas-pinduoduo-app-due-malware-issues-2023-03-21/

the company was able to create a comprehensive portrait of user's habits, interests and prefernces."[6]

33. According to cybersecurity experts, the Pinduoduo app is malware (short for malicious software) because it bypassed "user's cell phone security to monitor activity on other apps, check notifications, read private messages and change settings."[7]

34. Thereafter, the majority of the 100 or so engineers who had developed the exploits that collected user data without their permission were transferred to work for Temu.[8]

TEMU CONTAINS SPYWARE AND ACTIVELY COLLECTS USER INFORMATION

35. Through its marketing and advertisement, Defendant does not disclose and actively hide the existence of spyware on Temu users on its browser and cell phone applications.

36. More specifically, an analysis of the Temu software by multiple experts and reported by the market research company and short seller Grizzly Research, shows that Temu utilizes calls to outside device data and function that is inappropriate and dangerous.[9]

37. Compiling is the process of creating a computer executable from human-readable code. The Temu app contains "self-compiling software" that circumvents its user's phone's malware detection ability and allows Temu to illegally steal user data.[10]

38. Temu uses dynamic compilation using "runtime.exec()". Which calls for "package compile." This built in allows for unbounded use of exploitative methods.[11]

---

[6] Gan, Nectar, Yong Xiong and Juliana Liu. " 'I've never seen anything like this:' One of China's most popular apps has the ability to spy on its users, says experts." CNN. (April 3, 2023) https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html
[7] I.d.
[8] I.d.
[9] Grizzly Research. "We believe PDD is a Dying Fraudulent Company and its Shopping App TEMU is Cleverly Hidden Spyware that Poses an Urgent Security Threat to U.S. National Interests." (September 19, 2023).
[10] The Week. "Why shopping app Temu should be cause for consumer concern." https://theweek.com/china/1026408/temu-consumer-concern-china. (September 11, 2023).
[11] I.d.

39. Temu's Android cell phone version also intentionally fails to list many of the permissions of its source code in their Android manifest file. The permissions request for the following commands are not listed, despite being the most intrusive: CAMERA, RECORD_AUDIO, WRITE_EXTERNAL_STORAGE, INSTALL_PACKAGES, and ACCESS_FINE_LOCATION. [12]

40. Further, Temu is able to collect any and all files from the user's devices to send to their own servers, with little or no encryption.[13]

41. ACCESS_FINE_LOCATION is a permission for Temu records the precise location rather than the course location whenever the Temu app is running. Temu deceptively requests for users to grant the permission while a photograph is uploaded when an image search is conducted for similar listing.[14]

42. Temu also uses getWindow().getDecorView().getRootView(), to make screenshots and store screenshots as the user uses the smart phone, including the user's activities on other programs and data.[15]

43. Temu references access to the users' camera and microphone whenever the app is using.[16]

44. Temu records both the MAC address and the DNS address.[17]

45. The MAC address is a globally unique identifier of any device in any network, which can be used to identify the owner.[18]

---

[12] I.d.
[13] I.d.
[14] See 9.
[15] I.d.
[16] I.d.
[17] I.d.
[18] *Media Access Control Address (MAC Address)*, Techopedia (Nov. 18, 2014), available at https://www.techopedia.com/definition/5301/media-access-control-address-mac-address (last

46. Temu asks for the MAC address and inserts it into a JSON object to be sent to the server.

47. Temu seeks "root" access of the cell phone, which includes not only the files on the application, but all files on the device, including the programming of the other apps and the operating system.[19]

48. Temu's code references the system log files' address and options for shell commands.[20]

49. Temu obfuscates its app behavior through cleanup tools and debugger applications that makes it very difficult.[21]

50. Joe Security, an ISO 27001 certified company which specializes in the development of malware analysis systems for malware detection and forensics, rates Temu's app with 68/100, a score that is even higher than the malicious Pinduoduo app, which was suspended from the app store.[22]

51. Like their parent's malware, Pinduoduo, Temu's app is almost identically malicious in the categories: Spyware, Evader, and exploiter.[23]

USER DATA AND DATA BREACH

52. According to a September 13, 2023 NBC Chicago Report, entitled "Using TEMU could expose consumers to identity theft, other issues," the Better Business Bureau warns that "the app collects a lot of information from consumers, including your social media and banking information. Cyber security experts say they suspect the app could even bypass cellphone security

---

visited Nov. 8, 2022).

[19] I.d.
[20] I.d.
[21] I.d.
[22] I.d.
[23] I.d.

settings to spy on other apps and even change settings."

53. According to a September 15, 2023 CBS Chicago Investigation, entitled "Savings or Scam? BBB warns Temu takes personal info, citing hundreds of complaints," by Dorothy Tucker, the consumer group Better Business Bureau has issued a warning about Temu. Specifically, Temu "collects all kinds of information, from your name, phone number, and address to your birthdate, social media photos, and social security number." "It also automatically collects data from your phone, tablet, or laptop information like the operating system, browsing history, and location data."

54. Like many other online vendors, Temu requires customers to disclose personal identifying information and processes customer credit and debit card payments.

55. Temu application requests permissions including access to Bluetooth and Wi-Fi network information.

56. Temu application draws on customer data and search history with the assistance of artificial intelligence algorithms to discern emerging fashion preferences and patterns.

57. To aid in its data collection, Defendant's app also requests that users share their data and activity from other apps, including social media.

58. The BBB has amassed more than 900 complaints from consumers, including the unauthorized withdrawals from bank accounts and credit card purchases soon after the consumer began purchasing on Temu.

59. China's Cybersecurity Law, introduced in 2016 and enforced from 2017, obligates Critical Information Infrastructure (CII) operators to provide unobstructed access to their data to the government and mandates that such data be stored exclusively within mainland China.

60. Defendant's failure to comply with reasonable security standards provided Temu

with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of its own customers—including Plaintiffs and the Class members here—who have been subject to the Breach or have otherwise had their personal identifying information placed at serious and ongoing risk.

61. Temu allowed widespread and systematic theft of its customers' personal identifying information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' personal identifying information.

SECURITY BREACHES LEAD TO IDENTITY THEFT

62. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying information ("PII") to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[24] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records… [and their] good name."

63. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[25]

---

[24] *See* http:///www.gao.gov/new.items/d07737.pdf.

[25] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, alien registration number, government passport number, employer or taxpayer identification number." *Id*. (g)

64. A person whose PII has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

65. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[26] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other PII directly on various Internet websites, making the information publicly available, just as they have done here.

THE MONETARY VALUE OF PRIVACY PROTECTION

66. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.

67. Though Commissioner Swindle's remarks are more than two decades old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[27]

---

[26] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009).

[27] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited February 10, 2023) ("Web's Hot New Commodity: Privacy").

68. The FTC has also recognized that consumer data is a new—and valuable—form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[28]

69. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share—and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their PII.[29] This business has created a new market for the sale and purchase of this valuable data.[30]

70. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."

71. When consumers were surveyed as to how much they valued their personal data in terms of its protection against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access to their data at between $11.33 and

---

[28] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited February 10, 2023).
[29] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited February 10, 2023).
[30] *See supra*, n.4.

$16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[31]

72. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII, like Temu, has deprived that consumer of the full monetary value of the consumer's transaction with the company.

DAMAGES SUSTAINED BY PLAINTIFF AND THE CLASS

73. A portion of the services purchased from Temu by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiffs and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the Class incurred actual monetary damages in that they overpaid for the services purchased from Temu.

74. Further, as explained above, fraudulent use of PII might not be apparent for years, and consumers must expend considerable time and effort taking precautions to secure their PII for years to come.

75. In any event, as security blogger Brian Krebs notes, "credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts – such as credit and debit cards – and they're not great at stopping new account fraud committed in your name."

76. As a result of these activities, Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendant's wrongful conduct.

---

[31] Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited February 10, 2023); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011).

77. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

CLASS ACTION ALLEGATIONS

78. Plaintiff brings Count I and IV, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in the United States who registered an account with Temu at any time from July 2022 to the present day (the "National Class").

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

79. Plaintiffs bring Count II, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[32] who registered an account with Temu e-grocery service at any time from

[32] The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code § 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq.*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349,*et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania (73 P.S. § 201-1, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev.

> July 2022 to the present day (the "Consumer Fraud Multistate Class").

Excluded from the Consumer Fraud Multistate Class, are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

80. In the alternative to Count II, Plaintiff brings Count III, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of the following state sub-class, defined as:

> All persons residing in the State of New York who registered an account with Temu e-grocery service at any time from July 2022 through the present day (the "New York State Class").

Excluded from the New York State Class, are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers

81. The National Class, Consumer Fraud Multistate Class, and New York State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

82. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

NUMEROSITY

83. The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands to millions. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may

---

Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6- 101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

be ascertained from Defendant's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

COMMONALITY AND PREDOMINANCE

84. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Temu failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive personal information;

b. Whether Temu properly implemented its purported security measures to protect customer information from unauthorized capture, dissemination, and misuse;

c. Whether Defendant's conduct violates the New York and other asserted Consumer Fraud Acts;

d. Whether Defendant's conduct constitutes breach of an implied contract;

e. Whether Defendant violated the Federal Wire Tap Act, 18 U.S.C. §§ 2510, *et seq*.;

f. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

85. Temu engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

TYPICALITY

86. Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the Breach alleged herein. Further, there are no defenses available to Temu that are unique to Plaintiffs.

ADEQUACY OF REPRESENTATION

87. Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

INSUFFICIENCY OF SEPARATE ACTIONS

88. Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Temu. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

DECLARATORY AND INJUNCTIVE RELIEF

89. Temu has acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

SUPERORITY

90. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Temu, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS ALLEGED

CAUSES OF ACTION
COUNT I

Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq. (on Behalf of the National Class)

91. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

92. The Federal Wiretap Act, 18 U.S.C. §§ 2510, et seq., prohibits the interception of any wire, oral, or electronic communications without the consent. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communications is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

93. A "protected computer" under the CFAA includes any computer "which is used in

94. or affecting interstate or foreign commerce or communication." Id. § 1030(e)(2). Plaintiff's cellphone device is protected computer used in interstate commerce because it is connected to the internet. See United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) ("With a connection to the Internet, the … computers were part of a system that is inexorably intertwined with interstate commerce.").

95. "Intercept" is defined as the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

96. "Contents" is defined as "include[ing] any information concerning substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

97. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

98. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence, or any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…." 18 U.S.C. § 2510(12).

99. Defendant is a "person" for purposes of the Wiretap Act because it is a corporation.

100. Plaintiff's and Class Members' sensitive personal information and data were intercepted by Defendants through "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

101. Plaintiff and Class Members reasonably believed that Defendant was not intercepting, recording, or disclosing the electronic communications.

102. Plaintiff's and Class Members' electronic communications were intercepted during transmission, without consent and for the unlawful and/or wrongful purpose of monetizing private information and data, including by using private information and data to develop marketing and advertising strategies.

103. Defendant's actions were at all relevant times knowing, willful, and intentional, particularly because Defendant is a sophisticated party who knows the type of data it intercepts through its own products. Moreover, experts who uncovered the program injections have explained that the inclusion of the program injections were intentional, non-trivial engineering tasks—the kind that do not happen by mistake or randomly.

104. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by the interception, disclosure and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made by Defendant as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

105. Plaintiff and the other Class members suffered and will continue to suffer damages including but not limited to loss of their information and loss of money and costs incurred, all of which have ascertainable value to be proven at trial.

COUNT II

Violations of the Computer Fraud and Abuse Act, 18 U.S.C § 1030, et seq. (on Behalf of the National Class)

106. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

107. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

108. Defendant violated 18 U.S.C. 1030 by intentionally accessing Plaintiff's and Class Members' computers without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

109. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA.

110. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

111. Plaintiff's computer is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

112. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of programs downloaded to Plaintiff's computer, which is a protected computer as defined above. By storing sniffing code to access, collect, and transmits details of Plaintiff's web activities and communications, Defendants intentionally caused damage without authorization to those Class Members' computers by impairing the integrity of the computers.

113. Defendants violated 18 U.S.C. 1030(a)(5)(A)(ii) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such

conduct, recklessly caused damage to Plaintiff's and Class Members computers by impairing the integrity of data and/or system and/or information.

114. Defendants violated 18 U.S.C. 1030 (a)(5)(A)(iii) by intentionally accessing Plaintiff and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiff and Class Members.

115. Plaintiff and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

116. Plaintiff and Class Members have suffered loss by reason of these violations, as defined in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

117. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

118. As a result of these takings, Defendants' conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

119. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, the right of privacy.

120. Defendants' unlawful access to Plaintiff's and Class Members' computers and electronic communications has caused Plaintiff and Class Members irreparable injury.

COUNT III

Trespass to Personal Property/Chattels
(on Behalf of the National Class)

121. The common law prohibits the intentional intermeddling with a chattel, including an electronic device, in possession of another that results in the deprivation of the use of the chattel or impairment of the condition, quality, or usefulness of the chattel.

122. Defendant engaged in deception and concealment to gain access to the subject computers.

123. By engaging in the acts described above without the authorization or in excess of consent given by Plaintiff and other Class members, Defendant dispossessed Plaintiff and Class members from use and/or access to their computers, cellphone and/or online resources. Further, these acts impaired the use, value, and quality of Plaintiff's and Class members' computers and/or cellphones.

124. Defendant's acts constitute an intentional interference with the use and enjoyment of the subject computers and/or cellphones. By the acts described above, Defendant has repeatedly and persistently engaged in trespass to chattels in violation of the common law.

125. Defendant is liable to Plaintiff in an amount to be determined by the enlightened conscious of a jury for all compensatory, exemplary, and other damages proximately caused and/or flowing from Defendant's trespass to chattels.

COUNT IV

Violation of Section 349 of New York General Business Law
Deceptive Acts and Practices
(and Substantially Similar Laws of the Consumer Fraud States)
(on Behalf of the Consumer Fraud Multistate Class)

126. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

127. Defendants' actions alleged herein constitute unlawful, unfair, deceptive, and

fraudulent business practices.

128. Defendants' conduct constitutes acts, uses and/or employment by and/or their agents or employees of deception, fraud, unconscionable and unfair commercial practices, false pretenses, false promises, misrepresentations and/or the knowing concealment, suppression, and/or omission of material facts with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of services, and with the subsequent performance of services and transactions, in violation of section 349 of New York's General Business Law.

129. Defendants' acts and omissions were generally directed at the consuming public.

130. The unfair and deceptive trade acts and practices of Defendant have directly, foreseeably, and proximately caused damages and injury to Plaintiff and other members of the Class.

131. Defendants' violations of Section 349 of New York's General Business Law have damaged Plaintiff and other Class Members, and threaten additional injury if the violations continue.

132. Defendants' acts and omissions, including Defendants' misrepresentations, have caused harm to Class Members in that Class Members have suffered the loss of privacy through the exposure of the personal and private information and evasion of privacy controls on their computers.

133. Plaintiff and Class Members have no adequate remedy at law.

134. Plaintiff, on her own behalf, and on behalf of the Class Members, seeks damages, injunctive relief, including an order enjoining Defendants' Section 349 violations alleged herein, and court costs and attorneys' fees, pursuant to NY Gen Bus. Law § 349.

COUNT V

Unjust Enrichment
(In the Alternative to Count II and on Behalf of the New York State Class)

135. The common law prohibits Defendant from reaping a substantial financial profit at the expense of Plaintiff's and the other Class Members' expense without reasonable and equitable restitution.

136. Defendant reaped a significant financial profit from its system of monitoring the Internet connections on the subject computers or cellphones to provide targeted advertising and data harvesting without the consent of users.

137. Defendant monitors, tracks, and logs every browser connection made by users of the subject electronic devices.

138. Defendant assigns each installation of the subject software a unique machine and user identification code.

139. Every time a user attempts to access a website through a browser, the subject programs intercept the connection and re-routes it through a proxy that also sends user information to servers owned or controlled by Defendant.

140. Users of the subject electronic devices do not have a choice in participating in Defendant's business practices.

141. Defendant receives profit for this activity through a commission on purchases made at a merchant or selling data harvested during website users' interaction with the platform.

142. Defendant received substantial profits through the subject programs that Defendant would not have downloaded had Defendant properly disclosed the function and/or flaws in the subject programs.

143. Defendant was conferred a benefit in revenue that it would not have received from

Plaintiff for which it should equitably compensate Plaintiff and Class Members. Alternatively stated, Defendant was improperly enriched by its improper conduct and, under principles of equity, is required to compensate Plaintiff and other Class Members for Defendant's unjust enrichment.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Complaint so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually on behalf of himself and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Temu, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering Temu to pay actual damages to Plaintiffs and the other members of the Class;

C. Ordering Temu to pay for not less than three years of credit card monitoring services for Plaintiffs and the other members of the Class;

D. Ordering Temu to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

E. Ordering Temu to pay statutory damages, as provided by the New York Deceptive Acts and Practices Law and other applicable State Consumer Fraud Acts, to Plaintiffs and the other members of the Class;

F. Ordering Temu to disseminate individualized notice of the Breach to all Class members;

G. Ordering Temu to pay attorneys' fees and litigation costs to Plaintiffs and the other members of the Class;

H. Ordering Temu to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Dated: Flushing, NY
September 18, 2023

Respectfully submitted,
Attorneys for Plaintiffs
TROY LAW, PLLC

/s/ John Troy

John Troy, Esq.
Tiffany Troy, Esq.
Aaron B. Schweitzer, Esq.
41-25 Kissena Boulevard
Suite 110
Flushing, NY 11355
(718) 762-1324
troylaw@troypllc.com

CHUNG LAW FIRM, P.C.
James Chung, Esq.
43-22 216th Street
Bayside, NY 11361
(718) 461-8808
jchung_77@msn.com

SHEEHAN & ASSCOIATES, P.C.
Spencer Sheehan, Esq.
60 Cutter Mill Road
Suite 412
Great Neck, NY 11021
(516) 268-7080
spencer@spencersheehan.com